(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
15 juillet 2004 (15.07.2004)

PCT

(10) Numéro de publication internationale
WO 2004/059976 A3

(51) Classification internationale des brevets[7] :
H04N 7/167, H04L 9/08

(21) Numéro de la demande internationale :
PCT/FR2003/050202

(22) Date de dépôt international :
22 décembre 2003 (22.12.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
02 16650 24 décembre 2002 (24.12.2002) FR

(71) Déposant *(pour tous les États désignés sauf US)* : VIACCESS [FR/FR]; Les Collines de l'Arche, Tour Opéra C, F-92057 PARIS LA DEFENSE CEDEX (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : MERLE, Gilles [FR/FR]; 41 rue du Hameau, F-78480 VERNEUIL SUR SEINE (FR). BANGUI, François [FR/FR]; 69 rue Dunois, F-75646 PARIS 13ème (FR).

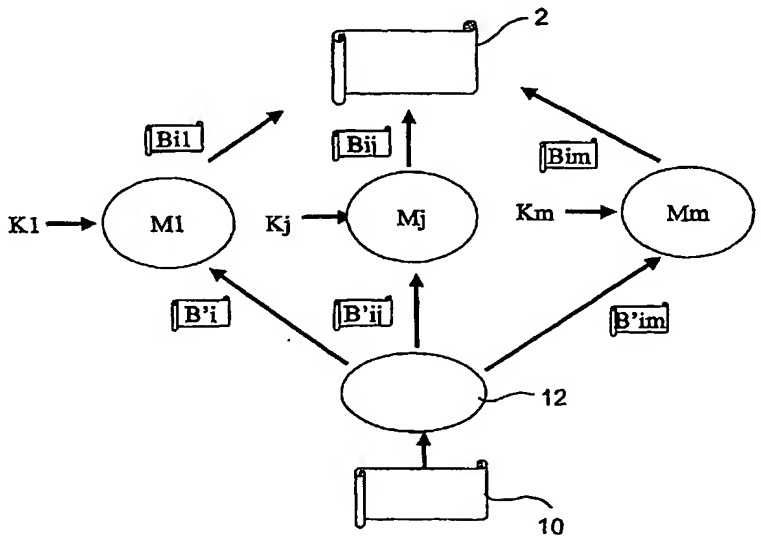
(74) Mandataire : POULIN, Gérard; c/o BREVALEX, 3 rue du Docteur Lancereaux, F-75008 PARIS (FR).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

[Suite sur la page suivante]

(54) Title: METHOD AND SYSTEM FOR SECURING SCRAMBLED DATA

(54) Titre : PROCEDE ET SYSTEME DE SECURISATION DE DONNEES EMBROUILLEES



(57) Abstract: The invention relates to a controlled-access method of distributing scrambled data to at least one receiving terminal. The inventive method involves a first encryption phase comprising the following steps consisting in: subdividing the data into a whole number of families Fj (j=1...M) each containing a whole number of blocks Bi (i=1...N); allocating a specific identification parameter pj (j=1...M) to each family Fj, said parameter being associated with at least one descrambling module Mj having a specific processing capacity and a specific security level; scrambling each block Bi of a family Fj of type pj with a key Kj (j=1...M) in a one-to-one relationship with parameter pj. The invention also involves a second descrambling phase comprising the following steps consisting in: identifying the family of each block Bi and descrambling each block Bi of a family of type pj with module Mj using key Kj.

[Suite sur la page suivante]

WO 2004/059976 A3

(84) **États désignés** *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *avec rapport de recherche internationale*

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

(88) **Date de publication du rapport de recherche internationale:** 19 août 2004

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) **Abrégé :** L'invention concerne un procédé de distribution avec contrôle d'accès de données embrouillées à moins un terminal récepteur. Le procédé selon l'invention comporte - une première phase de chiffrement comprenant les au étapes suivantes • subdiviser lesdites données en un nombre familles Fj (j=1...M) comportant chacune un nombre entier de blocs Bi (i=1 ...N) , • affecter à chaque famille Fj un paramètre spécifique d'identification pj (j=1...M) associé à au moins un module de désembrouillage Mj ayant une capacité de traitement et un niveau de sécurité spécifiques, • embrouiller chaque bloc Bi d'une famille Fj de type pj par une clé Kj (j=1...M) en relation biunivoque avec le paramètre pj, une deuxième phase de désembrouillage comportant entier de - et les étapes suivantes • identifier la famille de chaque bloc Bi, • désembrouiller chaque bloc Bi d'une famille de type pj par le module Mj au moyen de la clé Kj.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 03/50202

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N7/167 H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04N G06F H04H H04L G11B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	EP 0 984 630 A (MINDPORT BV) 8 March 2000 (2000-03-08) abstract column 1, line 1 - column 3, line 12	1-10, 17-19 11-16
Y	US 2001/053221 A1 (TAKEDA TSUNEHARU) 20 December 2001 (2001-12-20)	11-16
A	abstract paragraph '0005! - paragraph '0007! paragraph '0042! paragraph '0048! figures 11A-F,21	1-10, 17-19

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29 June 2004	15/07/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Post, K

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 03/50202

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 02/069638 A (CHAUBERT ERIC ;NAGRAVISION SA (CH)) 6 September 2002 (2002-09-06) abstract page 1, line 1 - page 3, line 19 page 5, line 15 - line 16 figures 1-3	1-19

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/FR 03/50202

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0984630 A	08-03-2000	EP 0984630 A1	08-03-2000
		JP 2000092045 A	31-03-2000
		ZA 9905259 A	21-02-2000
US 2001053221 A1	20-12-2001	JP 2002009757 A	11-01-2002
WO 02069638 A	06-09-2002	BR 0207581 A	27-04-2004
		CA 2438599 A1	06-09-2002
		EP 1374588 A1	02-01-2004
		WO 02069638 A1	06-09-2002
		US 2003133571 A1	17-07-2003

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 03/50202

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04N7/167 H04L9/08

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04N G06F H04H H04L G11B

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X Y	EP 0 984 630 A (MINDPORT BV) 8 mars 2000 (2000-03-08) abrégé colonne 1, ligne 1 - colonne 3, ligne 12	1-10, 17-19 11-16
Y A	US 2001/053221 A1 (TAKEDA TSUNEHARU) 20 décembre 2001 (2001-12-20) abrégé alinéa '0005! - alinéa '0007! alinéa '0042! alinéa '0048! figures 11A-F,21	11-16 1-10, 17-19

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
29 juin 2004	15/07/2004

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Post, K

Demande internationale No
PCT/FR 03/50202

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	WO 02/069638 A (CHAUBERT ERIC ;NAGRAVISION SA (CH)) 6 septembre 2002 (2002-09-06) abrégé page 1, ligne 1 - page 3, ligne 19 page 5, ligne 15 - ligne 16 figures 1-3	1-19

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No
PCT/FR 03/50202

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 0984630 A	08-03-2000	EP 0984630 A1	08-03-2000
		JP 2000092045 A	31-03-2000
		ZA 9905259 A	21-02-2000
US 2001053221 A1	20-12-2001	JP 2002009757 A	11-01-2002
WO 02069638 A	06-09-2002	BR 0207581 A	27-04-2004
		CA 2438599 A1	06-09-2002
		EP 1374588 A1	02-01-2004
		WO 02069638 A1	06-09-2002
		US 2003133571 A1	17-07-2003